Michael W. Sobol (State Bar No. 194857)
msobol@lchb.com
Roger N. Heller (State Bar No. 215348)
rheller@lchb.com
David T. Rudolph (State Bar No. 233457)
drudolph@lchb.com
Melissa Gardner (State Bar No. 289096)
mgardner@lchb.com
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Telephone: 415.956.1000
Facsimile: 415.956.1008

Attorneys for Plaintiffs

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

GREG JOHNS, LOLA HUNTER, YORKMAN LOWE, TIMOTHY MACK, and LEIGH DUNLAP, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

EQUIFAX, INC.,

Defendant.

Case No. 17-cv-5372

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

I. NATURE OF CLAIM

1. This action arises from a data breach at Equifax, Inc., which compromised the private, personal information of approximately 143 million people in the United States of America.

2. Defendant Equifax Inc. failed to safeguard and secure the sensitive personal information that it collects from nearly every American and later uses in a number of commercial applications. As a result, cyber attackers breached Equifax's data systems and exfiltrated the private information of nearly half the American population. The private information now in the hands of the cyber attackers includes immutable information, such as Social Security numbers, names, and dates of birth, as well as other sensitive information, such as addresses, driver's license numbers, employment data, credit card information, and security questions and answers used for verification to access private information on websites (collectively, personally identifying information, or "PII"). Equifax has also acknowledged that the data breached includes records relating to its function as one of the country's three primary credit reporting bureaus, i.e., more than 180,000 consumers' credit report "dispute documents."

3. The cyber attackers infiltrated data systems of Equifax in or about May 2017. For approximately 10 weeks thereafter, in May, June, and July of 2017, the cyber attackers maintained access to Equifax data systems, undetected. During this time, cyber attackers successfully exfiltrated massive amounts of PII of Americans from Equifax's data systems. Equifax has publicly stated that it discovered and stopped the data breach on or about July 29, 2017 (Herein, the "Data Breach.")

4. Not until September 7, 2017, approximately six weeks after it acknowledged it was aware of the Data Breach, did Equifax publicly disclose the Data Breach. During this time, Equifax deliberately kept the Americans who had their PII stolen from Equifax's systems in the dark about the Data Breach, including people who were paying customers of Equifax's identity protection services.

5. As a result of Equifax's failure to adequately secure its data systems and safeguard the PII of Americans that it possesses from and for commercial gain, Plaintiffs and the other

victims of the Data Breach will now perpetually face risks to the security and privacy of their personal affairs. On behalf of themselves and all others similarly situated, Plaintiffs seek damages, restitution, and injunctive relief for the proposed Class and California Subclass, as defined herein.

II. PARTIES

6. Each Plaintiff named herein has reason to believe, based upon the public reports of the Data Breach, its scale, and upon information provided by Equifax via its website, that his or her PII was taken during the Data Breach.

7. Plaintiff Greg Johns is a resident of Santa Clara County, California. On or about September 14, 2017, Plaintiff Johns visited the Equifax website which stated to him that he may be a victim of the Data Breach. On or about September 14, 2017, Plaintiff Johns initiated credit freezes with the three main credit report agencies, incurring costs therefor. Plaintiff Johns has devoted significant time to monitoring his accounts in response to the Data Breach.

8. Plaintiff Lola Hunter is a resident of Alameda County, California. On or about September 9, 2017, Plaintiff Hunter visited the Equifax website which stated to her that she may be a victim of the Data Breach. On or about September 9, 2017, Plaintiff Hunter signed up for an identity theft protection service, incurring costs therefor, and attempted to initiate credit freezes with the three main credit report agencies by phone, but as of September 15, 2017, Plaintiff Hunter has not received confirmation that her attempts to obtain credit freezes were successful. Plaintiff Hunter has devoted significant time to monitoring her accounts in response to the Data Breach.

9. Plaintiff Yorkman Lowe is a resident of Alameda County, California. On or about September 10, 2017, Plaintiff Lowe visited the Equifax website which stated to him that he may be a victim of the Data Breach. In or around May of 2017, Plaintiff Lowe learned that unauthorized charges had been made on his debit card, and expended time dealing with the ramifications of that fraud. Plaintiff Lowe has devoted significant time to monitoring his accounts in response to the Data Breach.

10. Plaintiff Timothy Mack is a resident of Kern County, California. On or about

September 8, 2017, Plaintiff Mack visited the Equifax website which stated to him that he may be a victim of the Data Breach. Plaintiff Mack has devoted significant time to monitoring his accounts in response to the Data Breach.

11. Plaintiff Leigh Dunlap is a resident of Los Angeles County, California. Plaintiff Dunlap has paid Equifax annually for credit monitoring and identity theft protection services for more than five years. On or about March 17, 2017, Plaintiff Dunlap paid Equifax $99.95 for an additional year of those services. Equifax did not provide Plaintiff Dunlap any information concerning the Data Breach at any time prior to publicly announcing the Data Breach on September 7, 2017. On or about September 8, 2017, Plaintiff Dunlap visited the Equifax website which stated to her that she may be a victim of the Data Breach. Plaintiff Dunlap has devoted significant time to monitoring her accounts in response to the Data Breach.

12. Defendant Equifax, Inc. is a Georgia corporation, registered with the California Secretary of State to do business in California, and headquartered in Atlanta, Georgia. Equifax purchased in 2013 and wholly owns a subsidiary, Trusted ID, Inc., a corporation headquartered in Palo Alto, California.

III. JURISDICTION AND VENUE

13. Pursuant to 28 U.S.C. § 1331, this Court has original subject matter jurisdiction over the claims of Plaintiffs and the Class that arise under the Credit Repair Organizations Act ("CROA"), 15 U.S.C. §§ 1679a *et seq.*

14. Pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005 ("CAFA"), this Court has subject matter jurisdiction over this putative nationwide class action because the matter in controversy exceeds $5,000,000.00, exclusive of interest and costs, and is a class action in which some members of the Class are citizens of states other than Equifax's state of citizenship. *See* 28 U.S.C. § 1332(d)(2)(A).

15. This Court has personal jurisdiction over Equifax because Equifax is authorized to do and does business in the State of California.

16. This Court has personal jurisdiction over Equifax because Equifax transacts substantial business in this judicial district.

17. Venue is proper in this Court under 28 U.S.C. § 1391 because, *inter alia*, Equifax regularly conducts substantial business in this district and is therefore subject to personal jurisdiction, and because a substantial part of the events giving rise to the Complaint arose in this district.

IV. INTRADISTRICT ASSIGNMENT

18. Venue is proper in this Division pursuant to Civil L.R. 3-2(c) because a substantial part of the events and omissions which give rise to the claim occurred in Alameda County.

V. FACTUAL BACKGROUND

A. Equifax Is In The Business Of Gathering Sensitive PII On A Massive Scale

19. Equifax operates as a credit bureau that compiles information about consumers' financial histories and provides it to, for example, creditors, landlords, and employers. Equifax has also become a large-scale aggregator of data for commercial exploitation, using the PII it collects about individuals to power a wide variety of data-driven products and services, operating in 24 countries, online, and in offices throughout the United States.[1]

20. In filings with the Securities and Exchange Commission, Equifax describes its business as follows: "We leverage some of the largest sources of consumer and commercial data, along with advanced analytics and proprietary technology, to create customized insights which enable our business customers to grow faster, more efficiently and more profitably, and to inform and empower consumers . . . Our revenue stream is diversified among businesses across a wide range of industries, international geographies and individual consumers."[2]

21. Equifax boasts that it is "home to comprehensive personal credit, employment and business data covering over 500 million consumers, 81 million businesses and employers as well as 250 million employees,"[3] and "the exclusive source for the most comprehensive workforce

---

[1] Jeff Pollard and Joseph Blankenship, *Equifax Does More Than Credit Scores*, FORBES (Sept. 8, 2017, 6:06 PM), https://www.forbes.com/sites/forrester/2017/09/08/equifax-does-more-than-credit-scores/#7e8a152819d8.

[2] *Fiscal Year 2016 Form 10-K* filed Feb. 22, 2017 by Equifax, at 29, S.E.C., https://goo.gl/ZZFBwA (last visited Sept. 15, 2017).

[3] *Industry Financial Services*, EQUIFAX, http://www.equifax.com/business/financial-services (last visited Sept. 15, 2017).

data available."[4] In total, Equifax claims to have data regarding more than 820 million individuals and more than 91 million businesses, worldwide.[5]

22. Equifax aggregates the PII of consumers it uses in its credit reporting and data aggregation business from multiple independent sources, including banks, credit card companies, public utilities, and housing providers. Equifax also aggregates employment data it obtains in connection with employment verification services it provides to prospective employers. In addition, Equifax aggregates data that government agencies provide in connection with regulatory compliance and other governmental functions, including data from the Supplemental Nutrition Assistance Program (SNAP), Temporary Assistance for Needy Families (TANF), Centers for Medicare & Medicaid Services (CMS), Department of Housing and Urban Development (HUD), Social Security Administration (SSA), Department of Labor (DOL) and Office of Child Support Enforcement (OCSE).

23. Equifax also collects information through a host of services sold directly to consumers with the promise that they can "take control of [their] financial life."[6] Some of these services include "Equifax® Identity Restoration," which provides access to a "dedicated restoration specialist" for help fixing inaccurate credit information, "Equifax ID Patrol™" and "ID Patrol™ Premier," which provide credit monitoring and financial alerts, the "Equifax Complete™ Family Plan," offering credit monitoring for up to four children,[7] "Equifax Debt Wise™" to help customers "get out of debt faster,"[8] "Complete™ Advantage Plan," offering to

---

[4] *Elevate Staffing*, EQUIFAX, http://www.equifax.com/business/staffing (last visited Sept. 15, 2017).

[5] *Company Profile*, EQUIFAX, http://www.equifax.com/about-equifax/company-profile/ (last visited Sept. 15, 2017).

[6] *Credit Report Assistance*, EQUIFAX, http://www.equifax.com/CreditReportAssistance/?/CreditReportAssistance (last visited Sept. 15, 2017).

[7] *A Surprise-Free Future Starts Here*, EQUIFAX, https://www.equifax.com/personal/identity-theft-protection (last visited Sept. 15. 2017); *Equifax Cybersecurity Incident*, EQUIFAX, https://help.equifax.com/s/article/ka137000000DRGPAA4/What-type-of-support-can-I-expect-with-Equifax-Identity-Restoration (last visited Sept. 15. 2017).

[8] *How Debt Wise Works*, EQUIFAX, http://www.debtwise.com/debt/how-debt-wise-works/en_dw (last visited Sept. 15, 2017).

enable consumers " to understand your credit and identity,"[9] and "Platinum Shield™," which Equifax says will allow purchasers to "[d]ecide who sees your Equifax credit file – and when they see it."[10]

B. Equifax Claims To Have State-Of-The-Art Information Security

24. Equifax calls itself "the trusted steward" of personal information.[11] It claims to have "state-of-the-art technology and the latest security standards in place."[12] On web pages directed to corporate clientele, for example, Equifax asserts that any corporate data provided to Equifax is hosted in "highly secure, state-of-the-art database facilities."[13]

25. On web pages directed to government agencies, Equifax states that it will "leverage" the "internal and disparate data resources," of government only with "the highest standards in security, privacy, quality and compliance,"[14] and encourages agencies to "[r]ely on [Equifax's] unmatched compliance, security, reliability and efficiency in data stewardship ensuring consistent and controlled access or release of your valued, sensitive data assets."[15]

26. On web pages directed to healthcare providers and payers, Equifax claims to abide by the principle that "providing information only to people with the appropriate credentials who have a legitimate right to access the information—is essential."[16]

27. An entity in Equifax's position, with access to the data consumers provide to

---

[9] *Your Next Step in Life Starts Now, It Starts Here*, EQUIFAX, https://www.equifax.com/personal/buying-a-car-or-home (last visited Sept. 15, 2017).

[10] *Platinum Shield*, EQUIFAX, http://www.equifax.com/cs/Satellite?pagename=comp (last visited Sept. 15, 2017).

[11] *Compliance*, EQUIFAX, http://m.equifax.com/consumer/fraud/compliance/en_us (last visited Sept. 15, 2017).

[12] *2005 Annual Report*, EQUIFAX, at 5, https://www.equifax.com/corp/investorcenter/annualReport2005/assets/pdfs/EFX_AR05_nar.pdf.

[13] *Data Management*, EQUIFAX, http://www.equifax.com/consumer/data_management (last visited Sept. 15, 2017).

[14] *Government Need—Leverage Analytics*, EQUIFAX, http://www.equifax.com/government/leverage-analytics (last visited Sept. 15, 2017).

[15] *Government Need—Manage my Workforce*, EQUIFAX, http://www.equifax.com/government/manage-my-workforce (last visited Sept. 15, 2017).

[16] *Healthcare—Trusted Secure Data Exchange Solutions*, EQUIFAX, http://learn.equifax.com/technology/anakam/solutions/healthcare/en_tas (last visited Sept. 15, 2017).

government, healthcare, employment, and financial services entities, holds a special position of trust, as Congress acknowledged when enacting the Fair Credit Reporting Act: "public confidence" in "credit reporting" is "essential to the continued function of the banking system," and credit reporting agencies "have assumed a vital role in assembling" consumer credit information and other information about consumers.[17]

28. Equifax amassed a tremendously valuable collection of sensitive information about the American public by representing to the people and entities who could provide such data—customers, corporations, employers, government agencies, and Congress—that Equifax was equipped to keep the data safe.

C. Equifax Knowingly Endangered The Information It Was Supposed To Protect And Exposed The PII Of Nearly Half The U.S. Population

29. As a result of being entrusted with the utmost sensitive personal and financial information of nearly all adult Americans, Equifax undertook a duty to keep that information safe. Equifax wholly breached this duty.

30. Equifax knew that because it holds the utmost sensitive PII of Americans, its systems are a target for ever-more sophisticated cyber attacks. Equifax emphasized this very point in a 2013 public press release referencing research by Javelin, Inc. regarding the unique value of PII in facilitating identity theft, and quoting Trey Loughran, president of the Personal Information Solutions unit at Equifax, stating, "Every day we hear more about the growing crime of identity theft . . . [but] many of us are not doing all that we can to help protect our identities."[18]

31. In recent years, hackers have repeatedly exploited flaws in Equifax's security, resulting in a nearly non-stop hemorrhaging of sensitive data. For example:

- In May 2016, Equifax's W-2 Express website suffered an attack that resulted in the leak of 430,000 names, addresses, Social Security numbers and other personal information provided to Equifax by the retail firm Kroger.[19]

---

[17] 15 U.S.C. § 1681.

[18] *Make Identity Theft Protection a Priority in 2014*, EQUIFAX (Dec. 31, 2013), https://investor.equifax.com/news-and-events/news/2013/12-31-2013.

[19] *Id.*

- In February 2017, Equifax "was forced to confess to a data leak in which credit information of a 'small number' of customers at partner LifeLock had been exposed to another user of [Lifelock's] online portal."[20]

- In March, April, and May of 2017, Equifax notified defense contractor giant Northrop Grumman and several other employers that employee W-2s stored by Equifax subsidiary TALX had been compromised in a series of data security incidents.[21]

32. Equifax failed to implement adequate security measures to safeguard the sensitive data it collected and stored, and willfully ignored known weaknesses in its data security, including but not limited to as revealed by prior hacks into its information systems. Equifax knew or should have known that its data security measures were insufficient, but failed to take adequate remedial measures to avoid future data breaches.

33. With respect to the recent Data Breach which is the subject of this lawsuit, Equifax states the hackers had exploited a "website application vulnerability" to gain access to the data.[22] A leading cyber security researcher, Brian Krebs, noted the exploitation of a vulnerability in an application indicates that Equifax had failed to properly apply updates to its Internet-facing Web applications.[23] Other experts reviewing Equifax's public-facing website, after the Data Breach was announced on September 7, have identified "common" vulnerabilities, "old" technologies, and out-of-date software that make the site particularly vulnerable to attack.[24]

34. Equifax also failed to implement adequate administrative controls to protect the sensitive information in its control. As Brian Krebs explains, "It's unclear why Web applications tied to so much sensitive consumer data were left unpatched, but a lack of security leadership at

---

[20] *Id.*

[21] Brian Krebs, *Fraudsters Exploited Lax Security at Equifax's TALX Payroll Division*, KREBS ON SECURITY (May 18, 2017, 4:23 PM), https://krebsonsecurity.com/2017/05/fraudsters-exploited-lax-security-at-equifaxs-talx-payroll-division/.

[22] *Equifax Announces Cybersecurity Incident Involving Consumer Information*, EQUIFAX, (Sept. 7, 2017), https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628.

[23] Brian Krebs, *Breach at Equifax May Impact 143M Americans*, KREBS ON SECURITY (Sept. 7, 2017, 6:30 PM), https://krebsonsecurity.com/2017/09/breach-at-equifax-may-impact-143m-americans/.

[24] Thomas Fox-Brewster, *A Brief History of Equifax Security Fails*, FORBES (Sept. 8, 2017, 8:40 AM), https://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-data-breach-history/#41a55795677c.

Equifax may have been a contributing factor."[25] Krebs reports that until "very recently," Equifax's role of "vice president of cybersecurity" was vacant.[26]

35. On September 13, 2017, Krebs exposed yet another security flaw on one of Equifax's public-facing websites: an online portal through which Equifax employees in Argentina manage credit report disputes from consumers in that country, and which contains hundreds of pages of complaints and disputes filed by Argentinians along with the Argentinian equivalent of Social Security numbers for thousands of people.[27] The information was protected from public access by only the easily guessed username and password combination: "admin/admin."[28]

36. Equifax's conduct following its tardy notification of the Data Breach also failed to meet basic security standards. In connection with the response, Equifax is requiring consumers to provide their PII to get additional information. The website that Equifax created for that purpose, and to notify people of the breach, runs on a stock installation WordPress, a content management system that doesn't provide the enterprise-grade security required for a site that asks people to provide their last name and all but three digits of their Social Security number. The Transport Layer Security (TLS) certificate, used to authenticate servers and clients and then use it to encrypt messages between the authenticated parties, reportedly does not perform proper revocation checks.[29] In the hours immediately following disclosure of the Data Breach, the main Equifax website was displaying debug codes, which for security reasons, is something that should never happen on any production server, especially one that is so close to so much sensitive data.[30]

37. Equifax's disregard for information security also manifests itself in the PIN numbers that it has provided for years to customers who contacted Equifax to place a security

---

[25] Krebs, *supra* note 23.

[26] *Id.*

[27] Brian Krebs, *Ayuda! (Help!) Equifax Has My Data!*, KREBS ON SECURITY (Sept. 12, 2017, 6:02 PM), https://krebsonsecurity.com/2017/09/ayuda-help-equifax-has-my-data/.

[28] *Id.*

[29] Dan Goodin, *Why the Equifax Breach is Very Possibly the Worst Leak of Personal Info Ever*, ARS TECHNICA (Sept. 7, 2017, 11:09 PM), https://arstechnica.com/information-technology/2017/09/why-the-equifax-breach-is-very-possibly-the-worst-leak-of-personal-info-ever/.

[30] *Id.*

freeze on their credit files. Consumers use credit freezes to protect themselves from identity theft, locking down their credit files and unlocking them only by using a PIN, with the goal of blocking identity thieves from being able to open credit lines in the consumer's name. As of September 10, 2017, when customers turned to Equifax to freeze their files, they were given a PIN number that could be cracked or re-generated easily by applying simple algorithms: the PIN consists of the date and time the freeze was requested, in MMDDYYHHMM format, such that a freeze requested September 10, 2017 at 2:15 p.m. would result in the PIN 0910171415.[31] According to reports, Equifax has used this approach to generate PIN numbers since at least 2007.[32]

D. Equifax's Slow And Opportunistic Response To The Data Breach Shows No Care Or Concern For Victims

38. Equifax's response to the Data Breach demonstrates indifference to the rights and concerns of the Americans whose information Equifax has "leveraged" for more than a century. Alarmingly, Equifax waited until nearly **six weeks** after the company first detected the massive extraction of consumers' PII, and **four months** after the company first had an *opportunity* to detect it—to make any public statement about the breach. On September 7, 2017, Equifax issued a press release. As of September 15, 2017, direct notice still has not been provided to the victims.

39. The delayed press release notice that Equifax issued on September 7, 2017, moreover, misled consumers about the information they could obtain by visiting the "dedicated website," (www.equifaxsecurity2017.com) that Equifax claimed would "help consumers determine if their information has been potentially impacted."[33] Equifax's website, which requires users to input six digits of their Social Security numbers to "see if your personal

---

[31] Ron Lieber, *After Equifax Breach, Here's Your Next Worry: Weak PINs*, N.Y. TIMES (Sept. 10, 2017), https://www.nytimes.com/2017/09/10/your-money/identity-theft/equifax-breach-credit-freeze.html; Mark Stockley, *Equifax: Woeful PINs Put Frozen Credit Files at Risk*, NAKED SECURITY BY SOPHOS (Sept. 10, 2017) https://nakedsecurity.sophos.com/2017/09/10/equifax-woeful-pins-put-frozen-credit-files-at-risk/.

[32] Tony Webster (@webster), TWITTER (Sept. 8, 2017, 7:38 PM), https://twitter.com/webster/status/906346071210778625.

[33] *Equifax Announces Cybersecurity Incident Involving Consumer Information*, EQUIFAX (Sept. 7, 2017), https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628.

information is potentially impacted,"[34] was being flagged by various browsers as a phishing threat. Rather than provide a yes or no answer to consumers querying whether their data was hacked, the site provided a message that credit monitoring services would be available for enrollment on a future date.[35] In some cases, people visiting the site were told they were not affected, only to find they received a different answer when they checked the site, with the same personal information, on their mobile phones.[36]

40. Customers who called the dedicated call center set up by Equifax were also unable to get answers. Several thousand consumers have described their experiences and concerns in comments on the Facebook page for Equifax, Inc. For instance:

> • Tried to enroll online. It's supposed to tell you if your info has been breached, then give you a date you can enroll. It did give me a date, 3 days from now, but DIDNT [sic] tell me if info has been compromised. If you do reach someone when you call, they can't or won't tell you anything. They said you have to wait until you enroll to find out. (Sept. 8, 2017)
>
> • Here's what they told me, "I'm just a third party - you have to call them directly- . . . . Call them directly." DID YOU even train this new call center? She also said this, "eeeequifax has some program you can enroll for a year. Call them directly" "I'm just an information line -third party taking heat for them. You can't sign up with me." She actually said the words "taking heat for them" - how crazy is that! (Sept. 8, 2017)
>
> • Neither your web site nor your number 1-866-447-7559 are working!!!!! When you click to continue enrollment process it takes you back to initial screen!!!! Your phone goes through the menu then hangs up!!! (Sept. 8, 2017)
>
> • Equifax hotline not helpful. Asked an operator named Diedre for assistance. She said "I can't help you." I asked for a supervisor and she hung up. Amazing. (Sept. 8, 2017)
>
> • They expanded call center hours and staff, but when you telephone on Saturday at 7:30am ET, you receive a recording saying our hours are 7am-1am ET, 7 days a week. You have called outside that time, and it disconnects you. (Sept. 9, 2017)

---

[34] *Cybersecurity Incident & Important Consumer Information*, EQUIFAX, https://www.equifaxsecurity2017.com/potential-impact/ (last visited Sept. 15, 2017).

[35] *Id.*

[36] Brian Krebs, *Equifax Breach Response Turns Dumpster Fire*, KREBS ON SECURITY (Sept. 8, 2017, 2:15 PM), https://krebsonsecurity.com/2017/09/equifax-breach-response-turns-dumpster-fire/.

- Don't bother calling Equifax. They are all reading from a script and won't help anyone AT ALL. I kept getting "ma'am we truly do apologize but we are unable to help you with your question." (Sept. 11, 2017)

- After three days of trying to get in touch with you I finally was able to and was disconnected by the agent. FIX.YOUR.PHONE!!!!! (Sept. 13, 2017)

- Additionally, when calling their call center, you will be asked if you would like to purchase further protection from Equifax. Unbelievable. (Sept. 7, 2017)[37]

41. Equifax's Data Breach website tells Americans they can claim a year of free credit monitoring through TrustedID, "[r]egardless of whether your information may have been impacted."[38] Equifax initially made no mention of the fact that TrustedID is owned and operated by Equifax.[39]

42. Equifax's response reveals its base opportunism, by positioning itself to offer Americans credit monitoring through "TrustedID," a wholly-owned Equifax subsidiary, in a transparent attempt to capture market share from its competitors and to increase its enrollment of customers who would pay for the service in later years.

43. On information and belief, Equifax stands to profit from the enrollment of victims who accept the "free" one-year offer. Using free "services as a means to introduce consumers to premium products and services" is a recognized business strategy and one that Equifax identified in its 2016 10-K filing with the Securities and Exchange Commission.[40] Indeed, much of Equifax's revenue growth has come from its sale of identity protection through TrustedID. Equifax noted in its Annual Statement to investors that it boosted revenue by 12% in 2013 due to increased sales of "U.S.-based subscription services," sales that were spurred by "the acquisition of TrustedID" in 2013.[41]

---

[37] Equifax (@Equifax), FACEBOOK, https://www.facebook.com/Equifax/ (last visited Sept. 15, 2017).

[38] EQUIFAX, *supra* note 34.

[39] *Equifax Buys TrustedID for $30 Million*, S.F. BUS. TIMES (July 9, 2013, 7:14 AM), https://www.bizjournals.com/sanfrancisco/morning_call/2013/07/equifax-buys-trustedid-for-30-million.html.

[40] S.E.C., *supra* note 2, at 16.

[41] *2013 Annual Report*, at 17, EQUIFAX, https://investor.equifax.com/~/media/Files/E/Equifax-

Footnote continued on next page

44. "Typically credit monitoring is free for a period of time, and then consumers are pitched purchasing additional protection when their free coverage expires."[42] Consistent with this common practice, the Terms of Service for TrustedID state that an individual's "membership subscription may be subject to automatic renewal."[43]

45. Offering credit monitoring to every American through TrustedID also positions Equifax to collect even more valuable PII. To sign up, a consumer must authorize TrustedID to retrieve information about the consumer from the other two credit bureaus (Experian and TransUnion). The information on the credit reports of the bureaus can vary significantly, meaning Equifax can gain access to, and ultimately profit from, additional information from the other two credit bureaus when consumers grant TrustedID access to their Experian and TransUnion credit files.

46. When consumers sign up for TrustedID, Equifax also requires a purported agreement to allow TrustedID to share their personal information with TrustedID's "affiliates"—which include Equifax Information Services LLC, a data brokerage arm of Equifax that sells consumer information, and which recently settled a lawsuit brought by the Federal Trade Commission over its allegedly unlawful selling of consumers' information to third parties who pitched predatory debt relief services to consumers in financial distress.[44]

47. Equifax's profit-driven purposes for offering TrustedID "protection" to breach victims finds additional support in the fact that Equifax has offered *no* protection for American children victimized by the Data Breach. Equifax knows that the PII of minors is in its databases,[45] and reports indicate that at least some minors under eighteen years of age were

---

Footnote continued from previous page
IR/Annual%20Reports/2013-annual-report.pdf (last visited Sept. 15, 2017).

[42] Krebs, *supra* note 23.

[43] *IDEssentials Terms of Use*, TRUSTEDID (effective Sept. 8, 2017) https://www.trustedid.com/serviceterms.php?serviceterms.

[44] *TrustedID Privacy Notice*, EQUIFAX, https://www.trustedid.com/premier/privacy-notice.php. (last visited Sept. 15, 2017); *FTC Settlements Require Equifax to Forfeit Money*, F.T.C. (Oct. 10, 2012), https://www.ftc.gov/news-events/press-releases/2012/10/ftc-settlements-require-equifax-forfeit-money-made-allegedly.

[45] *Minor Child Warning*, EQUIFAX, https://www.freeze.equifax.com/Freeze/jsp/SFF_FrzMinorChild.jsp (last visited Sept. 15, 2017).

affected by the Data Breach.[46]

48. Nevertheless, the Terms of Use for TrustedID effective September 8, 2017 specifically exclude minors from coverage, requiring consumers to purportedly agree that: "By registering for the Product You certify that You are at least 18 years of age."[47] The only explanation Equifax provides for this omission on its dedicated breach response webpage is, at best, incomplete and misleading. In response to the question "Can I sign up my minor child?," the site states: "Equifax does not typically have information associated with minors."[48]

49. Americans can *purchase* identity theft protection from Equifax for their children at a cost of $29.95 per month, however. Contrary to Equifax's representations in connection with the "free" trial membership offered to adult Data Breach victims, Equifax executive Trey Loughran stated in the 2013 press release that announced the Equifax Complete™ Family Plan that "[c]hild identity theft is a growing and often invisible problem,"[49] and Equifax answers the question "are my children at risk from identity theft?" in the affirmative on its website.[50] In video advertisements for its family plan, Equifax warns Americans that "child identity theft is on the rise, and it's important to protect your children as well as the adults in your household."[51] Indeed, recent studies suggest that close to one in ten children in America has had their Social Security number used by another person.[52]

---

[46] Kyle Clark & Jane Mo, *How Personal Information of Minors Could Be Compromised in the Equifax Breach*, KUSA-TV (Sept. 8, 2017, 6:21 PM), http://www.9news.com/news/local/next/how-personal-information-of-minors-could-be-compromised-in-the-equifax-breach/472467030.

[47] *TrustedID Premier Terms of Use*, EQUIFAX (effective Sept. 8, 2017), https://trustedidpremier.com/static/terms.

[48] *Cybersecurity Incident & Important Consumer Information*, EQUIFAX, https://www.equifaxsecurity2017.com/frequently-asked-questions/ (last visited Sept. 15, 2017).

[49] *Equifax Launches Identity Protection and Credit Monitoring Product for the Family*, EQUIFAX (Mar. 27, 2012), https://investor.equifax.com/news-and-events/news/2012/03-27-2012.

[50] *Are My Children at Risk From Identity Theft?*, EQUIFAX, https://www.equifax.com/personal/education/identity-theft/child-identity-theft (last visited Sept. 15, 2017).

[51] @Equifax, *Equifax Complete Family Plan*, YOUTUBE (May 14, 2014), https://www.youtube.com/watch?v=3CUdWxpCEo0.

[52] *Child Identity Theft Hits 1 in 10 Families*, Nat'l Credit Educ. Servs. (Mar. 27, 2015), http://ncesnow.org/child-identity-theft-hits-1-in-10-families/.

50. While Equifax's top executives kept their knowledge of the Data Breach to themselves, at least three such Equifax executives (including its Chief Financial Officer, President of U.S. Information, and President of Workforce Solutions), made unscheduled sales of their stock in the company worth about $1.8 million in total, cashing in on those assets before the upcoming drop in the value of Equifax stock that would inevitably follow those executive's strategically-timed disclosure of the Data Breach to the rest of America.

E. The Breach And Equifax's Response Harmed Plaintiffs And The Class

51. Plaintiffs and the other Americans victimized by the Data Breach are perpetually subject to a heightened risk of identity theft. The stolen PII may be used to open new financial accounts and incur charges or loans in victims' names, incur charges on existing accounts, or to clone ATM, debit, or credit cards. PII may also be used to commit other types of fraud including but not limited to immigration fraud, obtaining a driver's license or identification card in the victim's name, using the victim's information to obtain government benefits, filing a fraudulent tax return using the victim's information, assuming the victim's identity on social media, obtaining housing, jobs, and otherwise-unavailable medical prescriptions, damaging and destroying credit, and even committing crimes in victims' names.

52. As Senators Orrin Hatch and Ron Wyden stated in a September 11, 2017 letter to Equifax's CEO in the wake of the breach, in their capacity as members of the U.S. Senate Committee on Finance, "If the names, Social Security numbers, birth dates, and other information of 143 million Americans are now in the hands of cyber criminals, this breach will cause irreparable harm to programs within this Committee's jurisdiction by way of stolen identity refund fraud, healthcare fraud, and entitlement fraud."[53]

53. More than 15 million Americans had their identities stolen in 2016, costing them millions of hours of lost time and over $15 billion.[54] The U.S. General Accountability Office

[53] U.S. SENATE COMMITTEE ON FINANCE, Letter by Orrin Hatch and Ron Wyden (Sept. 11, 2017), https://www.finance.senate.gov/imo/media/doc/9.11.17%20Hatch,%20Wyden%20Request%20Information%20on%20Equifax%20Breach_Redacted.pdf.

[54] Identity Fraud Hits Record High, JAVELIN (Feb. 1, 2017), https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new.

(GAO) further reports that victims have "lost job opportunities, been refused loans, or even been arrested for crimes they did not commit as a result of identity theft."[55] As Equifax recently has advertised in connection with its direct-to-consumer credit monitoring and identity restoration services, "Experts report that a victim can spend anywhere from six months to two years recovering from identity theft."[56]

54. The unauthorized disclosure of Social Security numbers can be particularly damaging, because, like other immutable information such as name and date of birth, Social Security numbers cannot easily be replaced. The information exfiltrated in the Data Breach included such immutable PII of Americans, subjecting those victims to life-long heightened risks of identity theft, financial and other harm.

55. Plaintiffs and the other Americans victimized by the Data Breach will incur costs associated with time spent and the loss of productivity from addressing and attempting to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance, and annoyance of dealing with all issues resulting from the Data Breach, as well as damages to and diminution in value of their personal and financial information entrusted to Equifax.

56. Plaintiffs and the Class they seek to represent now face years of having to consistently monitor their financial, medical, and employment records, loss of rights, and potential problems securing housing, employment, credit, educational certifications, licensures, and other needs that could be compromised by criminals using the sensitive PII and other information that Equifax allowed to be stolen.

---

[55] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-14-34, Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent, at 11 (2013), *available at* http://www.gao.gov/assets/660/659572.pdf.

[56] *Learning Center Facts and Statistics*, EQUIFAX, https://web.archive.org/web/20101230104147/http://www.equifax.com/cs/Satellite/EFX_Content_C1/1172182371408/5-1/5-1_Layout.htm?packedargs=Locale%3Den_US (last visited Sept. 15, 2017).

VI. CLASS ACTION ALLEGATIONS

57. Plaintiffs bring this action, pursuant to Federal Rule of Civil Procedure 23, on behalf of themselves and the proposed Class and Subclass, defined as follows:

> **Class:** All persons residing in the United States and its territories whose personally identifiable information and/or financial information was breached as a result of the data breach announced by Equifax on or about September 7, 2017.
>
> **California Subclass:** All persons residing in the State of California whose personally identifiable information and/or financial information was breached as a result of the data breach announced by Equifax on or about September 7, 2017.
>
> Excluded from the Class and Subclass are Defendant; officers, directors, and employees of Defendant; any entity in which Defendant has a controlling interest; the affiliates, legal representatives, attorneys, heirs, and assigns of Defendant.[57]

58. The members of the Class and California Subclass are so numerous that the joinder of all members is impractical. While the exact number of Class and California Subclass members is unknown to Plaintiffs at this time, available reports indicate that the Class exceeds 100 million, and the Subclass is likely to be more than ten percent of the Class.

59. The proposed Class and Subclass are ascertainable, as determining inclusion therein can be accomplished through Equifax's own records.

60. This action satisfies the requirements of Federal Rule of Civil Procedure 23(b)(1)(A) because prosecuting separate actions by individual class members would create a risk of inconsistent or varying adjudications with respect to individual class members that would establish incompatible standards of conduct for Equifax.

61. This action satisfies the requirements of Federal Rule of Civil Procedure 23(b)(2) because Equifax's conduct in collecting data about consumers from both consumers and third parties, and then releasing that data to cyber criminals, were grounds generally applicable to members of the Class, and injunctive and declaratory relief would be appropriate respecting the Class as a whole.

62. This action satisfies the requirements of Federal Rule of Civil Procedure 23(b)(3) because it involves questions of law and fact common to each member of the Class that

[57] Plaintiffs reserve the right to amend the Class and Subclass definition if further investigation reveals that the Class should be expanded, divided into subclasses, or otherwise modified.

predominate over any questions affecting only individual members, including, but not limited to:

a. Whether Equifax knew or should have known that its computer systems were vulnerable to attack;

b. Whether Equifax breached a duty of care by failing to implement reasonable security measures;

c. Whether Equifax's conduct constitutes an unfair business practice under California's Unfair Competition Law (UCL);

d. Whether Equifax's conduct constitutes an unlawful business practice under the UCL for violating the Gramm-Leach-Bliley Act (GLBA);

e. Whether Equifax unlawfully used, maintained, lost or disclosed Class members' PII and other information;

f. Whether Equifax unreasonably delayed notifying affected customers of the Data Breach;

g. Whether Equifax failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Equifax's conduct was negligent;

i. Whether Equifax acted willfully and/or with oppression, fraud, or malice; and

j. Whether Plaintiffs and the Class are entitled to damages, restitution, civil penalties, punitive damages, and/or injunctive relief.

63. Plaintiffs' claims are typical of those of other Class members because Plaintiffs' PII, like that of every other Class member, was disclosed by Equifax in the Data Breach.

64. Plaintiffs will fairly and accurately represent the interests of the Class and California Subclass. Plaintiffs have retained counsel competent and experienced in both consumer protection and class action litigation. Plaintiffs' counsel has experience litigating other large data breach cases and complex consumer class actions, including numerous consumer class actions in the Northern District of California.

65. Class treatment is superior to any other method for adjudicating the controversy and this action may be reasonably managed and maintained as a class action under Rule 23(b)(3).

66. Even if Class members themselves could afford individual litigation, the court system could not. Given the complex legal and factual issues involved, individualized litigation would significantly increase the delay and expense to all parties and to the Court. Individualized litigation would also create the potential for inconsistent or contradictory rulings. By contrast, a class action presents far fewer management difficulties, allows claims to be heard which might otherwise go unheard because of the relative expense of bringing individual lawsuits, and provides the benefits of adjudication, economies of scale and comprehensive supervision by a single court.

FIRST COUNT
Negligence
(On behalf of the Class)

67. Plaintiffs incorporate the substantive allegations contained in all prior and succeeding paragraphs as if fully set forth herein.

68. Equifax knew or should have known the risks inherent to its possession of massive amounts of sensitive personal information, including that (a) hackers would target Equifax, as a dominant player in the consumer credit reporting and data aggregation industry, in order to acquire such information; (b) the risk of sophisticated cyber attacks was continual and increasing; (c) its own lax protocols had resulted in prior data breaches; (d) measures were available to adequately address its cyber security deficiencies; and (e) failure to implement adequate cyber security practices would result in a data breach.

69. By virtue of Equifax's unique position of power, responsibility, information, and trust by virtue of engaging in the business of soliciting and amassing the utmost sensitive personal information of Americans, Equifax owes a legal duty to Americans, including Plaintiffs and the Class, to keep that data safe and secure.

70. The Fair Credit Reporting Act creates a duty on behalf of Equifax, as a credit reporting agency, to safeguard the security of the data it obtains from Americans. 15 U.S.C. § 1681 *et seq.*

71. The Gramm-Leach-Bliley Act and associated regulations create duties on behalf of Equifax to insure the security and confidentiality of customer records and information and protect against hazards thereto including but not limited to unauthorized access or use, and to notify affected customers as soon as possible. 12 U.S.C. § 6801(b); 16 C.F.R. § 314.4.

72. Equifax owed a duty to disclose to Americans the material fact that its data security practices were inadequate to safeguard their personal information.

73. Equifax owed these duties, in particular, to Plaintiffs and the Class members, as persons whose PII and other information was in Equifax's possession.

74. Equifax had a special relationship with the Class because it was entrusted with their personal information. Equifax's ability to acquire Class members' PII and other information, from Class members and from other entities, created an independent duty of care because it was predicated on the understanding, including due to Equifax's own representations, that Equifax would take adequate security precautions.

75. Equifax breached its duties to Plaintiffs and the Class through its conduct alleged herein. Equifax had the ability to protect Class members' personal information from the cyber attack resulting in the Data Breach, but failed to do so. Equifax failed to implement reasonable or adequate data security practices to protect the type and scale of information in its possession, failed to timely detect the cyber attack, utilized outdated and otherwise improper security measures and techniques, failed to properly segment and patch systems containing sensitive consumer data, failed to disclose the flaws in its data security, and failed to provide timely notice of the Data Breach.

76. Equifax would have been able to prevent and/or limit the harm caused by the Data Breach had it maintained adequate protocols and security measures as alleged herein.

77. As a result of Equifax's breaches of its duties, Plaintiffs and the Class members have been injured as alleged herein.

78. The harm that Plaintiffs and the Class members have suffered and will suffer were foreseeable results of Equifax's conduct alleged herein. Equifax knew or should have known that its conduct would cause such harm.

79. Plaintiffs, on behalf of themselves and the Class, seek relief as prayed for below.

SECOND COUNT
Violation of Credit Repair Organizations Act, 15 U.S.C. §§ 1679a *et seq.*
(On behalf of the Class)

80. Plaintiffs incorporate the substantive allegations contained in all prior and succeeding paragraphs as if fully set forth herein.

81. Equifax is a "person" within the meaning of 15 U.S. Code § 1679b. Equifax is also a credit repair organization within the meaning of 15 U.S.C. § 1679a(3), because, among other things, it uses an instrumentality of interstate commerce or the mail to sell, provide, or perform (or represent that it will sell, provide, or perform) services in exchange for money or other valuable consideration for the express or implied purposes of advising and assisting consumers concerning their credit history, activity, record, and credit rating.

82. TrustedID is a credit repair organization within the meaning of 15 U.S.C. § 1679a(3), because, among other things, it uses an instrumentality of interstate commerce or the mail to sell, provide, or perform (or represent that it will sell, provide, or perform) services in exchange for money or other valuable consideration for the express or implied purposes of advising and assisting consumers concerning their credit history, activity, record, and credit rating.

83. The Credit Repair Organizations Act makes it unlawful to engage, directly or indirectly, in any act, practice, or course of business that constitutes or results in the commission of, or an attempt to commit, a fraud or deception on any person in connection with the offer or sale of the services of the credit repair organization, or to make or use any untrue or misleading representation of the services of a credit repair organization.

84. During the time that Equifax had knowledge of the Data Breach, but was withholding that knowledge from Americans, it engaged in misleading representations in connection with offering services for the purposes of advising and assisting consumers concerning their credit history, activity, record, and credit rating, including without limitation:

a. advertising and selling services that purported to allow consumers to "control" their financial lives;

b. advertising and selling services that purported to help consumers fix inaccurate credit information and "restore" their credit information;

c. advertising and selling services that purported to help consumers get out of debt;

d. advertising and selling services that purported to inform and alert consumers to unusual activity in connection with their personal and financial information;

e. advertising and selling services that purportedly allowed consumers to decide by whom and when their Equifax credit files would be seen; and

f. representing to governmental, corporate, and other entities providing information to Equifax, including consumers, that Equifax's cyber security was adequate to protect such information.

85. During the time that Equifax had knowledge of the Data Breach, but was withholding that knowledge from Americans, Equifax intentionally failed to disclose material facts, which it had a duty to disclose to them, concerning the existence, nature, and circumstances of the Data Breach.

86. During the time that Equifax had knowledge of the Data Breach, but was withholding that knowledge from Americans, Plaintiff Leigh Dunlap and other members of the Class paid Equifax or its affiliated or wholly-owned companies for services concerning their credit history, activity, record, and credit rating.

87. Equifax engaged in material misrepresentations or omissions of its services to induce Americans and certain members of the Class to enroll in Equifax's TrustedID credit services, for the purposes of obtaining further sensitive PII from such enrollees, and with the expectation that many such persons would renew their enrollment in TrustedID beyond the one-year free period, by:

a. affirmatively misrepresenting to consumers and the public that the dedicated Equifax breach website would inform individuals whether their information had been compromised in the Data Breach, when in fact the website provided, and provides, no meaningful answers but instead collects and stores users' names and Social Security numbers and puts them

on a waitlist to enroll with TrustedID;

b. omitting material information regarding TrustedID, including that it is a wholly-owned subsidiary of Equifax, and that registering for the service purported to waive an individual's right to pursue claims against Equifax or TrustedID in a court of law; and

c. affirmatively misrepresenting whether minors could have been affected by the Data Breach, including by expressly excluding them from coverage under the one-year trial offered through TrustedID and by making false statements on the dedicated breach website to the effect that Equifax does not store information concerning minors.

88. The above conduct was directed toward hundreds of millions of Americans, was frequent in terms of the nature of such noncompliance, and was intentional and intended to position Equifax to profit from Americans' reaction to the Data Breach.

89. As a result of Equifax's conduct alleged herein, pursuant to the Credit Repair Organizations Act, Equifax is strictly liable to the Class for all monies paid to Equifax by members of the Class under these false pretenses.

THIRD COUNT
Violation of California Customer Records Act, Cal. Civ. Code § 1798.80 *et seq.*
(On behalf of the California Subclass)

90. Plaintiffs incorporate the substantive allegations contained in all prior and succeeding paragraphs as if fully set forth herein.

91. The California Civil Code requires any "business that owns, licenses, or maintains personal information about a California resident [to] implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

92. Equifax owns, maintains, and licenses personal information, within the meaning of § 1798.81.5, about Plaintiffs and the California Subclass.

93. Equifax violated Civil Code § 1798.81.5 by failing to implement reasonable measures to protect the personal information of the members of the California Subclass.

94. The Data Breach occurred as a direct and proximate result of Equifax's violations of section 1798.81.5 of the California Civil Code.

95. Additionally, California Civil Code § 1798.82(a) provides that "[a] person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay. . . ."

96. Section 1798.2(b) provides that "[a] person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

97. Equifax is a business that owns or licenses computerized data that includes personal information as defined by Cal. Civ. Code § 1798.80 *et seq.*

98. In the alternative, Equifax maintains computerized data that includes personal information that it does not own as defined by Cal. Civ. Code § 1798.80 *et seq.*

99. The personal information (including but not limited to names, birth dates, and Social Security numbers) of the members of the California Subclass includes personal information covered by Cal. Civ. Code § 1798.81.5(d)(1).

100. Because Equifax reasonably believed that the personal information of the members of the California Subclass was acquired by unauthorized persons, it had an obligation to disclose the Data Breach in a timely and accurate fashion under Cal. Civ. Code § 1798.82(a), or in the alternative, under Cal. Civ. Code § 1798.82(b).

101. By failing to disclose the Data Breach in a timely and accurate manner, Equifax violated Cal. Civ. Code § 1798.82.

102. As a direct and proximate result of Equifax's violations of §§ 1798.81.5 and 1798.82 of the California Civil Code, Plaintiffs and the members of the California Subclass suffered the damages described above, including but not limited to time and expenses related to

monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their personal information.

103. Plaintiffs and the California Subclass seek relief under § 1798.84 of the California Civil Code, including, but not limited to, actual damages in an amount to be proven at trial, and injunctive relief.

104. Plaintiffs and California Subclass members are entitled to damages in an amount to be proven at trial.

FOURTH COUNT
Violation of the California Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200, *et seq.* ("UCL")
(On behalf of the California Subclass)

105. Plaintiffs incorporate the substantive allegations contained in all prior and succeeding paragraphs as if fully set forth herein.

106. As a result of Equifax's conduct alleged herein, the Plaintiffs have lost money or property within the meaning of the UCL.

107. Equifax violated the UCL by engaging in unfair, unlawful, and fraudulent business practices by its conduct alleged herein, including by, *inter alia*:

a. knowingly and recklessly maintaining deficient protocols and security measures that enabled cyber attackers to access the PII of the California Subclass members;

b. failing to adequately secure the utmost sensitive personal data of the California Subclass that was entrusted to and in the possession of Equifax;

c. failing to timely notify the California Subclass members that their PII and other information had been compromised in the Data Breach;

d. concealing and failing to disclose material information, including but not limited to information regarding the existence and nature of the Data Breach, the nature of Equifax's deficient cyber security practices, and the risks that such deficient practices posed to the California Subclass members;

e. making and disseminating affirmative misrepresentations regarding the nature of its security protocols and measures; and

f. directing California Subclass members to enroll in TrustedID services while concealing that TrustedID was a wholly-owned subsidiary of Equifax.

108. Equifax's conduct constitutes an "unlawful" business practice under the UCL. The Gramm-Leach-Bliley Act ("GLBA") mandates that financial institutions, such as Equifax, have an "affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." 15 U.S.C. § 6801. The GLBA requires such financial institutions to "develop, implement and maintain a comprehensive information security program" that is appropriate to the company's "size and complexity, the nature and scope of [the company's] activities, and the sensitivity of any customer information at issue."[58] Equifax failed to adopt appropriate security controls given Equifax's size and complexity, and the scope and sensitivity of the customer information that was at risk, in the manner mandated by the GLBA, 15 U.S.C. § 6801.

109. Equifax's conduct constitutes an unlawful business practice under the UCL by virtue of its violations of California common law, the California Customer Records Act, and the Credit Repair Organizations Act, as alleged herein, and by virtue of its violations of Cal. Civ. Code §§ 1770(a)(3), (7), (9), and (16).

110. Equifax's conduct alleged herein is immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers. There is no legitimate utility to Equifax's conduct alleged herein, and even if there were any utility, it would be significantly outweighed by the gravity of the harm to consumers caused by Equifax's conduct.

111. Equifax's conduct alleged herein is in contravention of California public policy, including but not limited to as such public policy is reflected in the California Customer Records Act and the Consumer Legal Remedies Act, Cal. Civ. Code §§ 1750 *et seq*.

112. Equifax's misrepresentations and omissions alleged herein are material in that a reasonable person would consider them important in making decisions.

---

[58] FTC Standards for Safeguarding Customer Information Rule, 16 C.F.R. § 314 (2017); *see also* September 8, 2017 Senate Committee on Commerce, Science, and Transportation letter to Equifax CEO Richard Smith.

113. Plaintiff Dunlap was deceived by and reasonably relied upon Equifax's material misrepresentations or omissions regarding its security practices in acquiring credit monitoring and identity theft services from Equifax and/or its affiliated companies.

114. Equifax's conduct alleged herein has a tendency to deceive reasonably objective consumers, including the members of the California Subclass.

115. As a result of the foregoing, Plaintiffs and the California Subclass members were harmed, including by, *inter alia*, paying money for services from Equifax, its affiliated companies, and other companies, taking other measures in response to the Data Breach, and by the increased risk that they will become victims of identity theft and other forms of fraud as described herein.

VII. PRAYER FOR RELIEF

WHEREFORE Plaintiffs pray for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiffs and their Counsel to represent the Class and California Subclass;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class members' PII, and other personal information, and from refusing to issue prompt, complete and accurate disclosures to the Plaintiffs and Class and California Subclass members;

C. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

D. For an award of actual damages, restitution, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined;

E. For an award of punitive damages;

F. For an award of costs of suit and attorneys' fees, as allowable by law; and

G. Such other and further relief as this court may deem just and proper.

Dated: September 15, 2017

Respectfully submitted,

LIEFF CABRASER HEIMANN & BERNSTEIN, LLP

By: */s/ Michael W. Sobol*
Michael W. Sobol

Michael W. Sobol (State Bar No. 194857)
msobol@lchb.com
Roger N. Heller (State Bar No. 215348)
rheller@lchb.com
David T. Rudolph (State Bar No. 233457)
drudolph@lchb.com
Melissa Gardner (State Bar No. 289096)
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Telephone: 415.956.1000
Facsimile: 415.956.1008

Attorneys for Plaintiffs

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a jury trial of their claims to the extent authorized by law.

Dated: September 15, 2017

Respectfully submitted,

LIEFF CABRASER HEIMANN & BERNSTEIN, LLP

By: */s/ Michael W. Sobol*
Michael W. Sobol

Michael W. Sobol (State Bar No. 194857)
msobol@lchb.com
Roger N. Heller (State Bar No. 215348)
rheller@lchb.com
David T. Rudolph (State Bar No. 233457)
drudolph@lchb.com
Melissa Gardner (State Bar No. 289096)
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Telephone: 415.956.1000
Facsimile: 415.956.1008

Attorneys for Plaintiffs